UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,890	09/28/2001	E. David Neufeld	COMP:0224	4334

7590 05/16/2008

Intellectual Property Administration
Legal Dept., M/S35
P.O. Box 272400
Ft. Collins, CO 80527-2400

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	**PAPER NUMBER**
2137	

MAIL DATE	DELIVERY MODE
05/16/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/966,890	NEUFELD ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *2/4/08*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-6,9-11,13-19,22-27,29-38 and 41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-6,9-11,13-19,22-27,29-38 and 41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the Applicant's Remarks and Amendments filed February 4, 2008.

Claims 1, 3-6, 9-11, 13-19, 22-27, 29-38, and 41 are pending and herein considered.

Response to Arguments

Applicant's arguments, with respect to the Examiner's 35 USC 101 rejection of claim 41 have been fully considered and re persuasive. The 35 USC 101 rejection of claim 41 has been withdrawn.

Applicant's arguments, with respect to the Examiner's 35 USC 112 rejection of claim 41 have been fully considered and are persuasive. The 35 USC 112 rejection of claim 41 has been withdrawn.

Applicant's arguments with respect to the Examiner's 35 USC 102(e) rejection of claims 1, 3-6, 9-11, 13-19, 22-27, 29-38, and 41 have been considered but are not persuasive.

The Examiner respectfully disagrees with Applicant's first set of arguments concerning Saarinen's alleged failure to disclose a state bit indicative of the state of the seed pool and examining that state bit or the position of a pointer to determine whether the seed pool is full as recited in claims 1 and 36. Calling attention once again to paragraphs 33 and 72, cited by the Examiner and re-cited by Applicant, the Examiner

would like to point out those portions within paragraph 72 that provide for “a predetermined value of input entropy" wherein the system checks to see if "sufficient input entropy has been stored" in which case the process continues onto the PRNG. Those familiar with the use of entropy pools to collect signals for use in generators are also familiar with the use of state bits and pointer positions in order to determine whether or not “sufficient input entropy has been stored.” The use of such means is not only common but the standard for determining whether or not a collection of information is sufficient for the intended purposes. As such, the Examiner maintains her rejection of claim 1 as given insofar as Saarinen clearly discloses setting a predetermined value, more than likely a state bit or pointer, in order to determine whether or not sufficient entropy has been stored.

The Examiner respectfully disagrees with Applicant’s next set of arguments concerning Saarinen’s alleged failure to disclose the writing of one or more bits to a seed pool altering a signature value and enabling the cryptographic security subsystem when more than a threshold portion of the signature value of the seed pool has been altered as recited in claims 13, 27 and 41. The Examiner would like to draw attention to paragraph 76 wherein Saarinen discloses the use of a counter variable and incrementing it by a constant between re-seeding processes in order to increase the security of the cryptographic system. It is the Examiner's position that the constant and counter of Saarinen serve as Applicant's signature value insofar as they are set but altered with the seeding of the pool so as to make it more difficult for attackers to gain access to the system. Additional support may be found in paragraph 55 wherein

Saarinen teaches the use of an output buffer to collect entropy bits and wherein Applicant begins by adding a constant C to the current counter variable T and placing the result in the output buffer. It is based upon these portions in view of the reference in its entirety that the Examiner maintains her position that Saarinen discloses the use of signature values within a seed pool, the altering of which may be used to signify to the cryptographic security subsystem that the seed pool has sufficiently been altered/filled and is ready to be used by the random number generator.

The Examiner respectfully disagrees with Applicant's next set of arguments concerning Saarinen's alleged failure to disclose establishment of the secure communication session if the plurality of data bits has at least a portion of the signature value as recited in claims 27. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., establishment of the secure communication session if the plurality of data bits has at least a portion of the signature value) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The Examiner respectfully disagrees with Applicant's next set of arguments concerning Saarinen's alleged failure to disclose disabling establishment of a secure communication session if the plurality of data bits has at least a portion of the signature value as recited in claim 27. The Examiner would like to briefly refer to those arguments above concerning Saarinen's disclosure of signature values, and the

enablement of a secure communications session once the signature value has been altered to show that sufficient entropy has been collected to seed the random number generator. Additionally, the Examiner would like to draw attention to paragraph 72 wherein Saarinen clearly states “If there is no sufficient accumulation of input entropy (i.e. a predetermined value of input entropy has not been stored), the process 510 continues to step 516 where entropy is further accumulated in the entropy pool” as distinguished from "if, on the other hang, sufficient input entropy has been stored, the process 510 continues to step 518 where the PRNG 104 is re-seeded." It is clear from these teachings that the sufficient accumulation of entropy bits, and associated altering of the bits signature value, in this case the constant and counter variable, is necessary in order for the establishment of a secure communication session, wherein a secure establishment of a secure communication session will not be able to proceed until sufficient entropy has collected. It is based upon these sections in view of the reference in its entirety that the Examiner maintains her position that Saarinen discloses disabling establishment of a secure communication session if the plurality of data bits has at least a portion of the signature value, i.e. sufficient entropy has not been collected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the

applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 3-6, 9-11, 13-19, 22-27, 29-38, and 41 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent Application Publication No. 2002/0172359 A1 to Markku-Juhani Saarinen, hereinafter referred to as *Saarinen*.

Regarding **claim 1**, Saarinen discloses a method of generating a cryptographic key for a cryptographic security subsystem of a processor-based device, the method comprising the acts of (a) detecting occurrence of a first type of triggering event (par 32); (b) writing one or more bits of data to a seed pool upon termination of the first type of triggering event, the seed pool comprising a state bit indicative of a state of the seed pool (par 32); (c) detecting occurrence of a second type of triggering event (par 32); (d) writing one or more bits of data to the seed pool upon termination of the second type of triggering event, wherein act (d) comprises masking one or more bits of data to the seed pool upon termination of the second type of triggering event (pars 27, 32, 33, 37, 42); (e) examining the state bit to determine whether the seed pool is full (pars 33, 72); and (f) if the seed pool is not full, repeating acts (a) through (e) until the seed pool is full (pars 33, 72); and (g) generating a pseudo-random number from the seed pool, wherein the pseudo-random number is used to generate a cryptographic key for the cryptographic security subsystem of the processor based device (par 27).

Regarding **claim 3**, Saarinen teaches wherein the first type of triggering event has a variable duration (pars 27, 32).

Regarding **claims 4-6**, Saarinen teaches wherein that the processor-based device is coupled to a communication link, and includes the act of receiving a communication from the communication link, the link comprising a plurality of types (pars 25, 27, 32, 33).

Regarding **claim 9,** Saarinen teaches wherein act (d) comprises capturing the one or more bits of data from a free-running timer upon termination of the second type of triggering event (pars 31, 32).

Regarding **claim 10**, Saarinen teaches wherein the second type of triggering event is different than the first type of triggering event (par 27, 32).

Regarding **claim 11,** Saarinen teaches wherein the second type of triggering event is a cycle of power applied to the processor-based device (pars 74-75).

Regarding **claim 13**, Saarinen discloses a method of initializing a seed pool for generating a cryptographic key for a cryptographic security subsystem of a processor-based device, the method comprising the acts of (a) prior to enabling the cryptographic security subsystem, writing a plurality of bits of data to a seed pool, the plurality of bits of data having a signature value (par 32); (b) detecting occurrences of a first type of triggering event (par 32); (c) writing one or more bits of data to the seed pool upon termination of the first type of triggering event, the one or more bits of data altering the signature value of the seed pool (par 32); and (d) enabling the cryptographic security subsystem when more than a predetermined portion of the signature value of the seed pool has been altered (pars 33, 72); and (e) generating a pseudo-random number from the seed pool, wherein the pseudo-random number is used to generate the

cryptographic key for the cryptographic security subsystem of the processor based device (par 27).

Regarding **claims 14 and 15**, Saarinen discloses wherein the first type of triggering event comprises either a cycle of power applied to the processor-based device or a reboot of the processor-based device (pars 25, 27, 32, 33, 74).

Regarding **claim 16**, Saarinen discloses wherein act (c) comprises the act of masking the one or more bits of data into the seed pool (pars 27, 32, 33, 37, 42).

Regarding **claim 17**, Saarinen discloses wherein act (c) comprises the act of capturing the one or more bits of data from a free-running timer (pars 25, 27, 31, 32, 33).

Regarding **claim 18**, Saarinen discloses detecting a second type of triggering event; determining if the seed pool is full; and writing one or more bits of data to the seed pool upon termination of the second type of triggering event if the seed pool is not full (pars 33, 72).

Claim 19 is directed towards a device's implementation of the method of claim 1 and is rejected by similar rationale.

Claim 22 is directed towards a device's implementation of the method of claim 3 and is rejected by similar rationale.

Claim 23 is directed towards a device's implementation of the method of claim 4 and is rejected by similar rationale.

Claim 24 is directed towards a device's implementation of the method of claim 5 and is rejected by similar rationale.

Regarding **claim 25**, Saarinen teaches wherein the interface controller comprises an RS232 interface controller (pars 25, 27, 32).

Claim 26 is directed towards a device's implementation of the method of claim 11 and is rejected by similar rationale.

Regarding **claim 27**, Utz discloses a processor-based device comprising: a host processing system, the host processing system comprising a processor (pars 25, 34); a communications management system in communication with the host processing system (pars 25, 34); a memory system in communication with the host processing system and the communications management system (par 25), wherein the communications management system comprises: an interface controller (pars 25, 26, 32); a non-volatile memory device to store a seed pool comprising a plurality of data bits (par 25, 28); and security logic in communication with the interface controller and the non-volatile memory device, the security logic configured to establish a secure communication session between the processor-based device and an external device in communication with the processor-based device via the interface controller (pars 25-26), and wherein the security logic is configured to: write one or more bits to the seed pool, wherein the one or more bits originate from a source external to the seed pool and alter a signature value (par 32); determine whether the plurality of data bits in the seed pool has at least a portion of a signature value (par 33) and disable establishment of the secure communication session if the plurality of data bits has at least a portion of the signature value (par 33).

Regarding **claim 29**, Saarinen discloses a main power supply to supply power to the processor-based device, and wherein the first type of triggering event comprises a cycle of the power supplied by the main power supply (pars 74-75).

Regarding **claims 30-31**, Saarinen discloses wherein the security logic is configured to detect a second type of triggering event; determine whether the seed pool is fully populated; and write one or more data bits to the seed pool upon termination of the second type of triggering event if the seed pool is not fully populated (pars 33, 72) and wherein the second type of triggering event comprises receipt of a communication from the external device via the interface controller (pars 25, 27, 32).

Regarding **claim 32**, Saarinen discloses wherein the interface controller comprises a network interface controller (pars 25, 27, 32).

Regarding **claim 33**, Saarinen teaches wherein the act of capturing one or more bits of data from a free-running timer upon termination of the first type of triggering event (pars 25, 27, 32).

Claim 34 is directed towards a device's implementation of the method of claim 33 and is rejected by similar rationale.

Regarding **claim 35**, Saarinen discloses wherein the security logic is configured to detect a first type of triggering event, and to write one or more data bits to the seed pool upon termination of the first type of triggering event (pars 25, 27, 32).

Regarding **claim 36**, Saarinen discloses a method for restoring security data to non-volatile memory in a computer system comprising: writing bits to a seed pool in discrete increments corresponding to a triggering event, wherein the seed pool is stored

in a portion of a non-volatile memory device (pars 32-33); tracking the state of the seed pool to determine if the seed pool is fully populated, wherein tracking the state of the seed pool comprises examining a state bit that changes states when the seed pool is fully populated or examining the position of a pointer to determine whether the portion of the non-volatile memory storing the seed pool is full (pars 33, 72); and precluding access to the computer system if it is determined that the seed pool is not fully populated (pars 33, 72).

Regarding **claim 37**, Saarinen further discloses wherein the triggering even comprises receipt of a query from a device external to the computer system (pars 25, 27, 32).

Regarding **claim 38**, Saarinen further discloses wherein writing bits to the seed pool in discrete increments corresponding to the triggering even comprises masking bits into the seed pool in discrete increments corresponding to a power cycle of the computer (pars 74-75).

Regarding **claim 41**, Saarinen discloses a method of manufacturing a processor-based device comprising: providing a memory comprising a seed pool, wherein the seed pool contains a plurality of bits having a signature value (par 33); writing one or more bits of data to the seed pool upon termination of a first type of triggering event (pars 25, 27, 32); and enabling a cryptographic security subsystem when more than a threshold amount of the signature value of the seed pool has been altered (par 33).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Tamara Teslovich/
Examiner, Art Unit 2137

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2137